AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Previously Presented) An automation security system, comprising:

an ~~plurality of~~ automation asset[[s;]] operatively coupled to a network communication channel, an automation asset comprises at least an automation control device and implements the following:

~~a plurality of remote devices or networks that utilize~~ an extensible factory protocol to transport data between ~~the plurality of~~ the automation asset[[s]] and ~~the plurality of~~ an automation asset on a remote network communication channel ~~devices or networks~~, the extensible factory protocol is a control-specific transport mechanism for data exchange between automation assets that encodes ~~utilize~~[[s]] at least one security field within the extensible factory protocol to exchange data with the remote automation asset, the security field of the extensible factory protocol authenticates at least one of a requestor of the data [[and]]or a supplier of the data. ~~, the security field provides at least one of a security parameter or a performance parameter, the factory protocol is dynamically changed or adjusted based upon considerations of desired security levels and real-time communications performance and employs lightweight or heavyweight encryption mechanisms based on the performance parameter~~.

2. (Currently Amended) The system of claim 1, the security field further comprises path information to ~~at least one of~~ identify a requester[[/]] or supplier of a connection~~, authenticate the requestor, and/or authenticate the supplier~~.

3. (Original) The system of claim 2, the path information facilitates non-connected data access by sending out an open-ended message.

4. (Currently Amended) The system of claim 1~~, the end-points include at least one automation asset,~~ the automation asset further comprises ~~includes at least one of~~ a controller, a

communications module, a computer, a sensor actuator, a network sensor, an I/O device, ~~a~~ Human Machine Interface (HMI), an I/O module, or [[and]] a network device.

5. (Currently Amended) The system of claim 1, the network communications channel is established across at least one of: a control network, factory network, information network, private network, instrumentation network, a wireless network, [[and]] or a public network.

6-8. (Canceled).

9. (Currently Amended) The system of claim 1, the extensible factory protocol ~~including~~ includes at least one of: a time component to mitigate replay attacks, a message integrity component, a digital signature, a sequence field to mitigate replaying an old packet, a pseudo random sequence, an encryption field, [[and]] or a dynamic security adjustment field.

10. (Currently Amended) The system of claim 1, the extensible factory protocol is adapted to at least one of: a Control and Information Protocol (CIP) or [[and .]]an object model that protects configuration of and transport of data between intelligent devices. ~~(Original)~~

11. (Currently Amended) The system of claim 1, further comprising a component to at least one of: provide source validation for identification, perform message digest checking for integrity checking, perform check sum tests, provide integrity mechanisms, provide encryption mechanisms, [[and]] or provide refresh security protocols.

12. (Currently Amended) The system of claim 1, the extensible factory protocol facilitates at least one of an identification, an authentication, an authorization, [[and]] or a ciphersuite negotiation to establish network trusts.

13. (Currently Amended) The system of claim 1, the extensible factory protocol is associated with a protocol supporting at least one of: a Temporal Key Interchange Protocol (TKIP) [[and]] or a wireless protocol.

14. (Currently Amended) The system of claim 1, the extensible factory protocol employing at least one of: an Elliptical function, an Aziz/Diffie Protocol, a Kerberos protocol, a Beller-Yacobi Protocol, an Extensible authentication protocol (EAP), an MSR+DH protocol, a Future Public Land Mobile Telecommunication Systems Wireless Protocols (FPLMTS), a Beller-Chang-Yacobi Protocol, a Diffie-Hellman Key Exchange, a Parks Protocol, an ASPeCT Protocol, a TMN Protocol, RADIUS, Groupe Special Mobile (GSM) protocol, [[and]] or a Cellular Digital Packet Data (CDPD) protocol.

15. (Currently Amended) The system of claim 1, the network communications channel employing at least one of: a Control and Information Protocol (CIP) network, a DeviceNet network, a ControlNet network , an Ethernet network , DH/DH+ network , a Remote I/O network, a Fieldbus network, ~~a Modbus network,~~ or a Profibus network.

16. (Original) The system of claim 1, further comprising a security field to limit access based upon line of sight parameters.

17. (Currently Amended) A method to facilitate factory automation network security, comprising:

determining network security requirements for automation devices of an industrial automation system including a requirement for real-time performance;

adapting a wireless security protocol for communication between automation devices of [[to]] the industrial automation system by lowering the security requirements if real-time performance is required;

employing the wireless security protocol ~~to communicate with~~ in communication between the automation devices of the industrial automation system; and

dynamically selecting a lightweight or heavyweight encryption mechanism based the network security requirements.

18. (Currently Amended) The method of claim 17, further comprising ~~encapsulating~~ incorporating a TKIP protocol within an automation protocol ~~in a TKIP protocol~~.

19. (Currently Amended) The method of claim 17, further comprising utilizing at least one of: a Temporal Key Interchange Protocol (TKIP) [[and]] or an Elliptical function in the wireless security protocol.

20. (Currently Amended) A method to facilitate automation network security, comprising:

determining a need for real-time communication with an automation control device;

establishing a communications session with [[an]] a remote automation ~~asset~~ control device across an automation control network *via* a heavyweight encryption mechanism in a security protocol employed in the communication session if real-time communications is not needed; and

exchanging data ~~with~~ between the automation ~~asset~~ control device and the remote automation control device in accordance with real-time communications *via* a lightweight encryption mechanism in the security protocol that induces minimal impact on [[a]] system[['s]] performance if real-time communication is needed.

21. (Currently Amended) The method of claim 20, further comprising dynamically switching between the heavyweight encryption mechanism ~~extended security protocol~~ and the lightweight encryption mechanism ~~security protocol~~ during the real-time communications.

22. (Currently Amended) The method of claim 20, the lightweight encryption mechanism ~~security protocol~~ includes at least one of: time component to mitigate replay attacks, a message integrity component, a digital signature, a sequence field to mitigate replaying an old packet, a pseudo random sequence, an encryption field, [[and]] or a dynamic security adjustment field.

23. (Canceled).

24. (Currently Amended) An automation security system, comprising:

means for encoding a security component within a factory protocol, the factory protocol is specifically adapted for data exchange between automation assets in a control domain and includes at least one of a security parameter or a performance parameter that is determined by at least one automation asset;

means for transmitting the security component and the factory protocol across a network between an automation asset in the control domain and an automation asset remote to the domain using a first standard of security if the at least one of a security parameter or a performance parameter dictates real-time performance is required, and a second standard of security if the at least one of a security parameter or a performance parameter dictates that real-time performance is not required, the first standard of security is lower than the second; and

means for the at least one automation asset to decode the security component in order to facilitate a secure communications channel across the network.

25. (Currently Amended) An automation security system, comprising:

~~an automation~~ a control device that utilizes an extensible factory protocol, the extensible factory protocol is implemented for data exchange between control devices across more than one communication network ~~for network communications~~;

a parameter detection component that detects at least one of a security or a performance parameter that extends the factory protocol, the factory protocol utilizes a lightweight encryption mechanism if real-time performance is required, a heavyweight encryption mechanism if the at least one of a security or performance parameter dictates that real-time performance is not required; and

an intrusion detection component adapted for the extensible factory protocol to detect network attacks directed to the ~~automation~~ control device.

26. (Original) The system of claim 25, the intrusion detection component is at least one of a host-based component and a network-based component.

27. (Currently Amended) The system of claim 25, the intrusion detection component is adapted to at least one of: an attack signature, an address, an address range, a counter, a location, a time, an event, a control list, a virus, or [[and]] a Trojan executable.

28. (Currently Amended) A security violation detection methodology, comprising:

adapting an industrial network protocol in accordance with an intrusion detection technology; and

monitoring the industrial network protocol for an attack *via* the intrusion detection technology, the monitoring is conducted at a first security level if real-time performance is requested between automation devices employing the industrial network protocol in remote networks, and a second security level if real-time performance is not requested, the first security level is lower than the second;

automatically performing a security action after detecting the attack, the security action includes at least one of enabling an alarm, denying network access or removing a virus.

29. (Original) The method of claim 28, further comprising monitoring a network for flooding attacks.

30-31. (Canceled).

32. (New) The automation security system of claim 1, the extensible factory protocol maintains backward compatibility with an automation asset incapable of implementing the security field.